REMARKS

Claims 1-12 are currently active.

Claims 7-12 have been added.

Claims 1 and 2 have been amended. Antecedent support for these amendments is found on page 33, line 25 and on page 35, line 27.

The Examiner has rejected Claims 1-6 as being unpatentable over Roger in view of Matyas. Applicants respectfully traverse this rejection.

Roger teaches that the increase in speed and efficiency of the Internet has not brought comparable increases in privacy and anonymity on the Internet. There are a number of motivations for the deployment of an anonymous publishing service. One of the goals of the teachings of Roger is pushing the world a few more steps in the direction of free and open information in communication. See page 1 of Roger. The teachings taught by Roger are for the purpose of providing tools to enable safer and more reliable communication for organizations fighting for increased rights of individuals rather than nations or corporations, as well as strengthening the capabilities of political dissidents and individuals to speak out anonymously about their situations. See the second paragraph of page 2.

Roger teaches the overall design is based on a community of servers where each server hosts data from the other servers in exchange for the opportunity to store data of their own. When an author wishes to publish a document, she breaks the document into shares, where a subset is sufficient to reconstruct the document. Then for each share, she negotiates for some server to publish that share on the community of servers, termed the servnet. The servers then trade shares around behind the scenes. When a reader wishes to retrieve a document from the servnet, she requests from any server, providing a location and key which can be used to deliver the document in a private manner. The server broadcasts the request to all other servers, and those which are holding shares for that document encrypt them and deliver them to the readers location. See page 5, last full paragraph.

Roger teaches the agents in the publication system are the author, the server, and the reader. Authors are agents that produce documents and wish to store them in the servers; servers are computers which store data for authors; and readers are users who retrieve documents from the service. The architecture of the system is based on a community of servers where each server hosts data from the other servers in exchange for the opportunity to store data of its own in the servnet. The servnet is dynamic: data moves from one server to another every so often, based partly on chance and partly on each servers trust of the others. Servers transfer data by trading. The only way to introduce a new file into the system is for a given server to use and thus provide more space on its local system. This new file will migrate to the servers by the process of trading. Each server has a public key and one or

more remail or reply blocks, which together can be used to provide secure, authenticated, pseudonymous communication with that server. Every machine in the servnet remembers information for some of the machines in the servnet. Only machines in the servnet are allowed to insert files into the network. The amount of storage space a given machine can use is limited by the amount of space it is willing to host. See page 55. Authors assign an expiration date to the documents when they are published; servers make a promise to maintain the availability of a given document until its expiration date is reached. The trust system is used to keep track of which of the servers are likely to keep this promise.

Roger teaches the structure of a server includes a control center which is located in the Haven module which performs the operations of training and trust. There is the Comm module which is responsible for communications with other servers and there is the node database which is a master list of all known servers and all known shares. These three modules are sufficiently distinctive. They are designed to run on separate community computers within an intranet. See page 56.

As is apparent from above, because of the context and the teaching of Roger, in regard to amended Claim 1, Roger does not teach or suggest the host computing device identifiable to the end user computing devices, nor the limitation that the n computing devices in the host computing device forming a trusted member list that each computing device has so each computing device knows the identity of the computing devices of the trusted peer-to-peer

network. Roger teaches the importance of anonymity between the servers of the servnet, and the last thing that Roger would want in regard to the servnet is for each of the servers to have knowledge and be able to identify all the servers of the servnet. In fact, because Roger teaches the need for anonymity, Roger teaches away from applicants' invention of Claim 1. It is this motivation of anonymity that drives the peer-to-peer architecture of the servnet with the requirement that any document must be split up into parts and distributed amongst the servers of the servnet to protect the identity of the author so the author would not be able to be identified, for instance, by a government agency, and be arrested. This context of Roger cannot be ignored. It is the basis and the key motivation that is behind the overall architecture of Roger which is contrary to applicants' invention of Claim 1, as amended.

Furthermore, as explained above, it is the reader who is the ultimate user who wishes to read the document that has been segmented into parts. When a reader wishes to retrieve a document from the servnet, she requests from any server, providing a location and key which can be used to deliver the document in a private manner. Thus, it is the reader, not even necessarily a member of the servnet who provides the key so the user can receive the document. It is the leader who does not have the digital signals who wishes to obtain the digital signals who provides the key. This is in direct contrast to the limitations of Claim 1 where the host computing device shares the digital signals with the two user computing devices and also sends a public key to a first of the two user computing devices.

Matyas teaches a key-management scheme based on control vectors. Matyas teaches a peer-to- peer environment is set up as follows: A serves keys to B or B serves keys to A. A key-distribution channel is first established from A to B, using nonelectronic methods. Applicants wish to emphasize this specific teaching found on page 84, second column of Matyas. By installing the keys using nonelectronic methods, it means that the keys are not sent by communication means between the computing devices. This teaching is also reiterated on page 185, first column wherein a different embodiment Matyas teaches that alternatively, key-distribution channels are first established from A to C and B to C using nonelectronic methods.

Furthermore, Matyas teaches that A serves a key to B by making a request for keys from C. in response, C generates a pair of keys and returns them to A, whereupon, A keeps one of the keys and serves the other to B. If C is permitted by the key distribution protocol to generate key encrypting keys for A and B, then C can be used to establish key distribution channels A to B and from B to A. Thereafter, A and B can use a peer-to-peer key distribution protocol provided they have a key generation capability. See page 185, column 1, first paragraph.

First, it should be pointed out that a pair of keys are returned to A, not a single key. Matyas teaches that A keeps one of the keys and serves the other to B. These are two different keys. In applicants' claimed invention. it is the same key that the host computer

sends to the first of the two user computing devices and the first user computing device sending a public key to a second of the two user computing devices through the communication means to establish the decentralized trusted network. That is, all the computing devices of the trusted and decentralized peer-to-peer network have the same public key so they all can communicate with each other in applicants' claimed invention. This is contrary to the teachings of Matyas where different keys are provided to A and B, thus limiting the ability for the different parties in Matyas to be able to communicate with each other. This is stated by Matyas wherein Matyas teaches that thereafter, A and B can use a peer-to-peer key distribution protocol so that there can be key distribution channels from A to B and from B to A, but C is not mentioned as part of the channels or the protocol. Thus, this is another distinction in the applied art of record from the limitations of Claim 1. Moreover, nowhere does the Matyas teach a host computing device which both transmits the digital signals to the two user computing devices as well as the host computer sending a public key to the first of the two user computing devices.

It is the Examiner's contention that the combination of Roger and Matyas arrive at applicants' invention of Claim 1. Applicants respectfully traverse this rejection. There must be some teaching or suggestion in the applied art of record itself to combine the teachings the Examiner is relying upon to arrive at applicants' claimed invention, and here, there is none. In fact, it is respectfully submitted that the Examiner is using hindsight to arrive at applicants' claimed invention. The Examiner is using the limitations of Claim 1 as a roadmap

to attempt to find the different limitations in Roger and that Matyas, and having supposedly found them, concluding that applicants' claimed invention is arrived at. This is not the law.

Besides the fact that the applied art of record fails to teach or suggest many of the limitations of Claim 1, separately or together, there is no reason why one skilled in the art would ever consider combining the teachings of Roger with the teachings of Matyas. Their contexts are completely different. Roger requires there to be anonymity between the servers of the servnet and specifically teaches the reader provides the key. In contrast, Matyas specifically by implication requires each of the parties A, B and C to know each other and for C to generate the key. However, there is no teaching or suggestion whatsoever that C also wants to obtain documents that have been split up into many different parts and distributed throughout the servnet. Accordingly, Roger and Matyas has no relevance or reason to be combined with each other, let alone to arrive at applicants' invention of Claim 1.

Accordingly, the applied art of record does not teach or suggest sending a public key through the communication means to the user computing devices, nor does the applied art of record teach sending the same public key from the host computing device to a first of the two user computing devices and the first user computing device sending the same public key to a second of the two user computing devices, nor does the applied art of record teach a host computing device that both sends the digital signals to the two user computing

devices and sends the public key to the first of the two user computing devices. Consequently, applicants' Claim 1 is patentable over Roger in view of Matyas.

Claim 2 is patentable for the reasons Claim 1 is patentable. Claims 3-6 are dependent to parent Claim 2 and are patentable for the reasons Claim 2 is patentable.

The Examiner has rejected Claims 1-3 as being unpatentable over Olson in view of Matyas. Applicants respectfully traverse this rejection.

Referring to Olson, there is described a method for performing client-hosted application sessions in distributed processing systems. Each client maintains its own copy of application data throughout the application session. Each of the plurality of clients can communicate with one another via the network 12. When a client initiates a new game application session, that client is referred to as the host client. It is the host client that is responsible for managing the environment under the distribution of application data between the clients participating in the application session that takes place. See column 6, lines 42-45. The host client assigns a unique identifier to the client that is requesting admission into the application session. Each client within the session will have its own system player ID. Once the host client has notified all of the participants in the application session of the addition of the new client, the host client processor precedes to program step 48. At that functional step, the host downloads the then current application data to the newly admitted client.

Olson teaches the use of a session key is passed down to each client with the name table portion of the application data. The session key is a random number which allows the host to generate non-predictable, non-repeating player ID's for new players so that clients in the session do not reuse player ID's. This session key has nothing to do with a public key, as found in Claim 1. See column 11, lines 21-34. Olson teaches that in the event that player 3 at client C effects a change in the game state, it will change its own corresponding application data stored at location 24. Client C will simultaneously compete that change via network 12 to each of the other clients and the application session using a peer-to-peer messaging scheme. See column 13, lines 7-16. It is respectfully submitted, from the description above regarding Olson, that it has nothing to do with a trusted and decentralized peer-to-peer network. While there is a peer-to-peer network mentioned, it is certainly not trusted in the sense that there are no public keys even identified or taught by Olson. Furthermore, there is absolutely no teaching or suggestion of a host computing device that both shares digital signals with the two user computing devices and also sends a public key to a first of the two user computing devices.

Olson in combination with Matyas also fails to arrive at applicants' claimed invention. Matyas has been discussed in detail above, and all of its deficiencies regarding the limitations of Claim 1 are certainly not met by Olson.

Not only does the combination of Matyas and Olson fail to meet many of the limitations of Claim 1, but there is absolutely no reason why one skilled in the art would combine the teachings of Matyas with the teachings of Olson. Olson's specific context is in regard to a group of computer gamers playing a game together. Olson does not teach or suggest the need whatsoever of having to have any type of encryption key to provide for a secure gaming session. As explained above, the Examiner is simply using applicants' limitations in Claim 1 as a roadmap to attempt to find these limitations in Matyas and Olson, and then conclude that applicants' invention of Claim 1 is arrived at. This is not patent law. There must be some teaching or suggestion to combine the teachings the Examiner relies upon in Matyas and Olson, and there is none; nor can the Examiner use hindsight to arrive at applicants' claimed invention as a motivation to combine Olson and Matyas.

Accordingly, Claim 1 is patentable over the combination of Olson and Matyas. Claim 2 is patentable for the reasons Claim 1 is patentable over the applied art of record. Claims 3-6 are dependent to parent Claim 2 and are patentable for the reasons Claim 2 is patentable.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 1-12, now in this application be allowed.

Respectfully submitted,

ARTHUR R. HAIR, ET AL.

By _____
Ansel M. Schwartz, Esquire
Reg. No. 30,587
One Sterling Plaza
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
(412) 621-9222

Attorney for Applicants

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 6/7/06

_____
Ansel M. Schwartz
Registration No. 30,587